G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Workshop Briefing Paper

2018

SHAPING RESPONSIBLE STATE BEHAVIOR IN CYBERSPACE

BRUNO LÉTÉ AND PETER CHASE

Please direct inquiries to:
The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

This publication can be downloaded for free at http://www.gmfus.org

The views expressed in GMF publications and commentary are the views of the author alone.

The publication is the product of the partnership between The German Marshall Fund of the United States and Microsoft.

About the Authors

Bruno Lété currently is a senior fellow at The German Marshall Fund of the United States in Brussels, where he works on security and defense policy.

Peter Chase is a resident senior fellow at The German Marshall Fund of the United States in Brussels, where he works on the transatlantic economy with particular attention to trade and investment, digital and energy policies, and the EU's relationship with third countries.

About The German Marshall Fund of the United States

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

Cover photo credit: Natali_Mis / Sutterstock.com

SHAPING RESPONSIBLE STATE BEHAVIOR IN CYBERSPACE

2018

BRUNO LÉTÉ AND PETER CHASE

INTRODUCTORY NOTE:

In February 2017, at a major IT security conference in San Francisco, Microsoft President and Chief Legal Officer Brad Smith presented arguments for a "Digital Geneva Convention," and a month later presented the case to Europeans at GMF's Brussels Forum. As an organization dedicated to promoting transatlantic cooperation in the spirit of the Marshall Plan — that is, based on the values of respect for the dignity of the individual, democratic political processes, market-based economies, and the rule of law — GMF was interested in understanding how Europeans thought about the idea of developing binding international law to constrain nation states' ability to engage in cyber-attacks. In this light, GMF organized in partnership with Microsoft a series of off-the-record roundtable discussions in Berlin, Paris, and Warsaw involving top government officials, lawyers, academics, corporate leaders (including from non-IT companies), and civil society to explore the issue. The following report is based upon both those discussions and GMF's own research.

Executive Summary

Concerns about cybersecurity have sky-rocketed as governments, economies, and societies increasingly depend on the Internet while the number of cyber-attacks expands. While hackers, organized crime, and terrorist organizations are all part of the threat environment, nation-states have far greater financial and technical capabilities to wreak havoc through cyber-attacks. Ensuring that existing law or a new international agreement clearly binds nation states to responsible behavior in cyberspace remains a worthy goal to strive for, although it seems difficult to achieve in the current international climate. However, our discussions in Warsaw, Paris, and Berlin showed a clear desire to continue to explore avenues that commit countries to respect laws, rules, or norms in cyberspace. As a priority, more time must be given to the United Nations Group of Governmental Experts to meet in different formats and to agree on the key issues that divide nations. Parallel efforts, undertaken by smaller bodies such as the Organization for Security Cooperation in Europe (OSCE) or the Organization for Economic Cooperation and Development (OECD), can create an additional layer of opportunities by pledging member states to respect guidelines or declaring their joint intent. Setting ambitious goals remains key, even if step-by-step progress and the gradual acceptance of norms, rather than large-scale negotiations, is likely to present the best method to move forward and create more safety and transparency in cyberspace.

The deep divisions among governments around the world also suggest the need to create flexible and more workable coalitions among like-minded nations. In Europe, there is reason for optimism. Key capital cities such as Paris, Berlin, and Warsaw are aligned in their interests and ambitions. This "Cyber Weimar Triangle" along with other like-minded member states such as the U.K., Netherlands, and Estonia constitute a driving force inside the European Union toward a united EU vision on how to deal with state-sponsored attacks in cyberspace. Europe's unity provides it the chance to lead by example, and to translate a European vision on state behavior in cyberspace across other global fora, including the OSCE or the United Nations. The fact that the EU is trying to bolster its cooperation with NATO gives cause for hope that a transatlantic alignment of interests is within reach in the cyber defense domain as well.

Finally, building trust and cooperation between governments and the private sector remains a key element of enhancing our cybersecurity. Tech companies are uniquely positioned to identify lacunas in existing or new standards, regulation or agreements. As such, nation states have the responsibility to remain open-minded about ideas emerging from the private sector that advance transparency and accountability in cyberspace. Initiatives, such as Microsoft's Digital Geneva Convention, may seem too ambitious, but by identifying the shared responsibility governments and companies bear to keep cyberspace safe, and the prominence this effort has brought to the issue, it fulfills a real need.

Our eight recommendations in this report all point to intensifying dialogue on these various issues, starting first with smaller efforts among like-minded governmental and nongovernmental actors. The challenge for decision-makers and legislators will be to transform these ideas into practical processes, and to find the political will to implement them.

1. Do not give up on the United Nations Group of Governmental Experts — patience is necessary and a variety of formats is helpful.

2. Experiment with other platforms — the OECD and OSCE offer good options.

3. A rigid, binding agreement may look ideal — but accepting (some) flexibility might be more realistic.

4. Create an NGO for cyberspace whose core task will to be attributing cyber-attacks.

5. Dissuasion and countermeasures matter — an international coalition willing to act will make irresponsible behavior more costly.

6. The private sector is responsible for creating more security in cyberspace — but so are governments.

7. Private sector ideas like the Digital Geneva Conventions fulfill a need — but do not let the name distract from the substance.

8. Educate civil society — use it as a driving force in international cyber diplomacy.

Part I: Problems and Solutions

Over the past two decades, rapid advances in computers, software, communications, and sensing technologies have connected billions of individuals across the globe, integrated economies through connected supply chains, and spurred new efficiencies through the Internet of Things, all the while stimulating additional new technologies and ways of doing things that have brought untold advances in health, education, agricultural production, economic growth, and general human welfare.

These advances however also bring challenges, including the now nearly-absolute dependence of developed and many developing countries on the integrity of our digital networks and systems. Despite the general resilience of network-based systems, deep digital integration has also created new vulnerabilities to cyber-attacks by individual hackers, organized crime, terrorist groups and even nation states.

Of these threats, rogue governments intending harm are perhaps the greatest. Public and private sector experts work continuously to mitigate the risks of cyber-attacks but are continuously tested by governments that can bring immense financial, technical, and military resources to develop new cyber tools to exploit product or human vulnerabilities that are inevitable in any complex system. An attack by one government intentionally seeking to bringing down the financial, energy, or other systems of another country could provoke untold economic damage and potentially extensive loss of civilian life.

> *"An attack by one government intentionally seeking to bringing down the financial, energy, or other systems of another country could provoke untold economic damage and potentially extensive loss of civilian."*

These attacks, unfortunately, are all too real. Starting with the Russian denial of service attacks on the Estonian government and financial system in 2007, the attacks have gotten more numerous and more destructive: the "WannaCry" ransomware attack of May 2017 affected hundreds of thousands of computers in 150 countries. The "NotPetya" attack a month later, which the United States publicly attributed to Russia, was deemed by the White House to be the most expensive cyber-attack in history. These two attacks are the most frequently discussed, but there have been at least 67 other significant cyber incidents between NotPetya in June 2017 and April 2018.[1]

Seeking Solutions

Devastated by the two world wars of the last century, governments developed a framework of international law and organizations to try to avoid war, and to constrain the actions of governments when war is waged. These efforts are epitomized by the Geneva Conventions as re-written after World War II, and in particular the Fourth Geneva Convention which establishes protections for non-combatant civilians in times of war. While experience over the past seven decades has sadly demonstrated that the instruments of international law do not stop governments from even mass genocide against innocent civilians, that legal framework sets necessary standards against which actions by governments can be judged, condemned, and eventually even punished by the international community, acting in accordance with the law.

A relatively small body of specialized law applies to cyberspace, including in particular the 2004 Budapest Convention on Cyber Crime as well regulations adopted by the International Telecommunications Union.[2] Existing legal instruments, however, may not be sufficient when cyber warfare almost necessarily affects — and indeed, must be executed through —the privately-owned and operated digital networks which are the foundation of modern economies and societies.

[1] See Center for Strategic and International Studies, Significant Cyber Incidents Since 2006, last updated April 2018.

[2] Anthony Rutkowski, The Digital Geneva Convention Exists, Just Use It, CircleID, December 16, 2017.

Probably the most significant of the efforts to clarify the application of existing legal frameworks is the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which has run in five sessions since it was set up in 2004. The Third UN GGE in 2013 agreed that international law is applicable to state behavior in the information and communications technologies (ICT) area, and that the rights and obligations that flow from the concept of sovereignty apply. Critically, it also found that "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."[3] More significantly, the Fourth UN GGE Report, which was endorsed by the General Assembly, reaffirmed the application of international law to cyberspace and reaffirmed that states, in their use of ICTs, must respect international law, including with respect to state sovereignty. It further recognized the right of states to "take measures consistent with international law," implicitly recognizing the right to take countermeasures in response to a cyber-attack.[4] Unfortunately, however, the Fifth UN GGE broke down in mid-2017, as Cuba, fronting for countries such as China and Russia, argued against the previously acknowledged rights to take countermeasures in self-defense (against an attack or provocation) and against the application of international humanitarian law to cyber warfare.[5] With no clear path out of this current deadlock, prospects for a Sixth UN GGE remain unclear for now.

> *"The UN GGE and the Tallinn Manuals provided the intellectual bedrock for other major efforts to give expression to international law in cyberspace that have come since."*

A further critical effort has been the "Tallinn Manual"[6] developed under the auspices of the NATO Cooperative Cyber Defense Centre of Excellence (CCD-COE) between 2009 and 2013 as well as the "Tallinn Manual 2.0,"[7] published in February 2017. In these manuals, groups of highly reputed international legal experts thoroughly reviewed a wide range of treaties, including the Geneva Conventions, as well as court judgments and indeed state practice to explore the application of international law to cyber warfare, in terms of norms governing the use of force by nation states (*jus ad bellum*), the conduct in armed conflict (*jus in bello*), the application of international humanitarian law and, in Tallinn Manual 2.0, activities that fall below these thresholds.[8]

The in-depth studies of the UN GGE and the Tallinn Manuals provided the intellectual bedrock for other major efforts to give expression to international law in cyberspace that have come since, including the G-20 communiqués of 2015[9] and 2016,[10] the G-7 Communiqué of 2017,[11] and civil initiatives such as the Internet Government Forum, and the Global Commission on the Stability of Cyberspace (GCSC), established by the Global Conference on Cyber Security in 2015.

These efforts, however important, have fallen short of a workable agreement. If there is a general recognition that international law applies to cyberspace, the failure of the UN GGE in 2017 underscores there is no consensus about how or when it applies. Even NATO governments have openly disagreed with some of the most fundamental concepts detailed in the Tallinn Manuals, with

[3] The Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, June 24, 2013.

[4] The Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, July 22, 2015.

[5] See, e.g., Michael Schmitt and Liis Vihul, International Cyber Law Politicized: The UN GGE's Failure to Advance International Norms, Just Security, June 30, 2017.

[6] Michael Schmitt, editor, et al, *The Tallinn Manual on The International Law Applicable to Cyber Warfare*, April 2013, Cambridge University Press.

[7] Michael Schmitt, *The Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations*, March 2017, Cambridge University Press.

[8] While these explorations were advised by outside observers, including NATO's Allied Transformation Command, the U.S. Cyber Command, and the International Committee of the Red Cross (which has a special role in the implementation of international humanitarian law), they reflect the views only of the legal experts who engaged in the deliberations.

[9] See G20 Leaders' Communiqué, Antalya Summit, November 15–16, 2015.

[10] See G20 Leaders' Communiqué, Hangzhou Summit, September 4–5, 2016.

[11] See G7 Taormina Leaders' Communiqué, Taormina Summit, May 26–27, 2017.

ranking officials in the U.S. Department of Defense legal team recently arguing that the "principle" of sovereignty does not have the force of a primary rule of international law, and as such does not prohibit attacking the civilian infrastructure of another state "provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention."[12] Similar ambiguity exists over numerous other issues, including when states are permitted to use force (the thresholds below an armed attack), the definition of "armed force," the application of international law to non-state actors (often acting at the behest of a government), the level of "permissible" doubt allowed before undertaking an attack that might affect civilians, and indeed the respective application of international humanitarian and/or human rights law.[13]

Further, most of these efforts were not sufficiently advised by the IT sector, which — in one of the novelties of cyber warfare — is on the front lines in the event of a cyber-attack by a nation state and which also plays an essential role in the critical issue of uncovering the source of a cyber-attack, which can much more easily be hidden than is the case for conventional attacks.

In part to bring a more technological voice into the debate, Microsoft proposed in February 2017 in the United States[14] and the next month in Europe[15] six principles which should inform international law on cyber warfare and could be embedded in a legally-binding "Digital Geneva Convention," including:

- A prohibition on targeting private sector and critical infrastructure;

- An obligation to assist private sector efforts to contain, respond to, and recover from state-sponsored attacks;

- An obligation on governments to report discovered vulnerabilities in programs to private sector developers;

- An obligation to exercise restraint on developing cyber weapons;

- A commitment to non-proliferation of such weapons; and

- An obligation to limit offensive operations to avoid mass civilian events.

A slightly more detailed Microsoft Policy Paper introduces a number of additional ideas, including protection of journalists, protections against "back doors" into consumer devices, prohibitions on industrial espionage, etc.[16] Microsoft has further called for a new international organization that brings together governmental and private sector experts to investigate and share evidence to attribute cyber-attacks to responsible governments.[17]

Part II: Reactions

Against this backdrop, The German Marshall Fund of the United States organized three roundtables between February and May 2018, in Warsaw, Paris, and Berlin — the "Cyber Weimar Triangle" — bringing together in each city national politicians, ranking officials from the ministries of foreign affairs (including the cyber policy directors and legal advisors) and defense, professional, and academic specialists in international law, representatives of both the IT and non-IT industries, and some others from civil society to solicit European views on the application of international law to state behavior in cyberspace. The discussions were off the record to facilitate frank conversation.

In the end, the discussions in all three cities covered similar territory, although with differences in emphasis, as will be discussed below. All participants agreed that state-based cyber-attacks are a real and growing problem, as over 30 countries are known to possess offensive cyber capabilities. This will get worse, as disruptive cyber technology is relatively

[12] See, for instance, Michael Schmitt, "In Defense of Sovereignty in Cyberspace," Just Security, May 8, 2018, reacting against "Sovereignty in the Age of Cyber" by the Staff Judge Advocate of U.S. Cyber Command, Colonel Gary Corn and former Department of Defense Office of the General Counsel attorney Robert Taylor, who argue, inter alia, that the principle of sovereignty "does not establish an absolute bar against ... state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention."

[13] Derek Jinks, "Understanding the Fog of War: Enduring Ambiguities in International Security Law," Just Security, May 30, 2018.

[14] Brad Smith, "The Need for a Digital Geneva Convention," On the Issues, Microsoft Corporation, February 14, 2017.

[15] Brad Smith, "Introduction to Plenary Session 8 on Transatlantic (In-Security)," The German Marshall Fund of the United States, Brussels Forum 2017, March 25, 2017.

[16] Microsoft Policy Papers, "A Digital Geneva Convention to Protect Cyberspace," April 2017.

[17] Microsoft Policy Papers, "An Attribution Organization to Strengthen Trust Online," Microsoft, April 2017.

easy to develop, leading to a kind of "democratizing" of weapons of mass destruction. The danger of states, especially larger belligerent ones, developing and using cyber weapons, was seen by all as qualitatively different from even organized crime. Although organized crime can also devote substantial resources to this area, it is more interested in robbery and extortion than undermining economies as a whole. Not surprisingly, the sense of threat was substantially higher in Warsaw, which has had some direct experiences and knows all too well the problems attacks have caused its Baltic and Ukrainian neighbors.

> "There is caution to avoid anything that might undermine the hard-won victory in the UN that international law applies to state behavior in cyberspace."

There was also nearly universal agreement among participants in all three countries that international law applies to state behavior in cyberspace, and in that sense strong support for the UN GGE conclusions and the work (if not necessarily all the details) in the Tallinn Manuals. A few participants also stressed the important of a little-known but potentially powerful concept in international law, the "Martens Clause," that stipulates that "… in cases not covered by the law in force, the human person remains under the protection of the principles of humanity and the dictates of the public conscience." In effect, this means that acts of states cannot be considered legal or permissible simply because they are not explicitly prohibited. This concept arguably fills any major holes in existing law as it applies to cyber-attacks by states.[18]

There was some worry that a "Digital Geneva Convention" could open opportunities to weaken existing statutes. Despite approving the underlying concept in Berlin, Paris, and Warsaw there is caution, especially among those most familiar with the issue, to avoid anything that might undermine the hard-won victory in the UN that international law applies to state behavior in cyberspace. Directly related to this was the oft-expressed tactical concern that Russia and China in particular would use any attempt to negotiate a new international legal instrument on state behavior in cyberspace to broaden the agenda to cover their proposals on "information security," which essentially justifies domestic controls over free speech and access to information from third countries. These two led naturally to the third major concern, that negotiating a new treaty would be laborious, could actually weaken existing legal constructs as encapsulated by the UN GGE and the Tallinn Manuals, and might never succeed.

In all three capitals there was furthermore repetitive concern about the ambiguities in international law and thus debate about its actual scope. Part of this, of course, is related to the fact that the rules on the use of force and armed attack were written well before current digital technologies were developed. However, participants argued that these ambiguities are not significant, and that the law is clear. Governments on both sides of the debate are intentionally raising doubts, in part to give themselves flexibility to act, some academic experts in all three cities argued. [19] The law of state responsibility, for instance, was said to clearly ascribe to the state full responsibility over illegal attacks emanating from its territory (and through its telecommunications infrastructure), such that governments cannot argue that they are not responsible for actions by nongovernmental groups, whether or not under their control (this effectively broadens the principles enunciated by the UN GGE).

There is more murkiness around the role of the private sector. Everyone acknowledged that the private sector is uniquely affected by state-based behavior in cyberspace — in many countries, the telecommunications infrastructure may be privately owned or operated, and internet platforms and software are overwhelmingly so. In this sense,

[18] See for example, Peter Asaro, *Jus Nascendi*, Robotic Weapons and the Martens Clause, in Ryan Calo, Michael Froomkin and Ian Kerr (eds.) *Robot Law*, Edward Elgar Publishing, 2016.

[19] U.K. Attorney General Jeremy Wright, in an otherwise admirable speech meant to clearly outline the U.K. government's views on the application of international law to cyberspace, essentially argued this in a May 23, 2018 speech after our roundtables, where he supported the U.S. Department of Defense lawyers' afore-mentioned contention that the principle of sovereignty does not prohibit offensive actions that do not rise to a "prohibited intervention," that is, one that is coercive on another state. Jeremy Wright, Cyber and International Law in the 21st Century, Government of the United Kingdom, Attorney General's Office, May 23, 2018.

attacks may well go through the private sector, and the private sector will be the first called on to respond. In addition, potential targets of cyber-attacks — financial companies, the energy sector, etc. — will frequently be private sector. Finally, given the likelihood that any attack may spread well beyond its intended target (as did both WannaCry and NotPetya), civilian collateral damage has been and will be frequent. The impact on "non-combatants" and the issues this raises under International Humanitarian Law (including the Geneva Conventions) was not discussed in depth, although many noted that cyber-attacks will normally fall below the threshold of armed hostilities that trigger the application of that body of international law. In its absence, international human rights law (including as implied through the Martens clause mentioned above) may be more appropriate.

Another issue that was raised and discussed at length in all three cities was that of attribution. International law allows a state to use force and/or take countermeasures against another state if the targeted state has first violated its international obligations. But to do so, and to have one's own actions considered legitimate, the problem being addressed has to be clearly attributed to the other state. This can be exceptionally difficult in the case of cyber-attacks, especially if conducted by non-state "proxy" parties, as has usually been the case. In this sense, participants were interested in learning more about existing digital forensic technologies, their reliability in pin-pointing the source and how the public and private sectors can interact in this area.

Finally, a few participants questioned the industry's interest in raising the issue of cyber-attacks to the level of international law, not least to protect itself from liability in the event of cyber-attacks using vulnerabilities in its software (as happened most spectacularly for Microsoft in the case of the WannaCry attack). More discussion would be needed on the obligation of states not to stockpile vulnerabilities they detect and to inform software vendors about these vulnerabilities accordingly — indeed, some have argued the U.S. government bears some responsibility for WannaCry for not having alerted Microsoft sooner to the weaknesses in the software. But all stressed the responsibility of all players in cyberspace to practice good cyber-hygiene, and of governments and IT equipment and software suppliers to educate their citizens on this.

Part III: Recommendations

The state-sponsored cyber-attacks of the past years are a wake-up call. They surface a number of questions for governments on what shape the World Wide Web should take in the future and how cyberspace can be more transparent and better regulated. For the private sector too, the increase in state-sponsored cyber-attacks generates critical questions on how to engineer products that are safe and adhere to software quality assurances.[20] Even though these cyber-attacks rarely rise to the level of a clear act of aggression, the rapid increase in their scope and sophistication increasingly puts ordinary civilians in the line of fire. The public and private sectors bear shared responsibility to define policies to protect citizens from cyber-attacks orchestrated by nation states. While critiques of the specific idea of negotiating a new "Digital Geneva Convention" may abound, so too does support for the idea of strengthening international law and trying to "shape responsible state behavior in cyberspace." Participants at our roundtables suggested a number of possible steps, which we have integrated with our own thoughts below.

1. Do not give up on the United Nations Group of Governmental Experts — we need patience and a variety of formats.

A global system like the World Wide Web needs global agreement to be effectively regulated. The United Nations Group of Governmental Experts is still the best tool available in this respect, and has been able to present important recommendations regarding responsible state behavior in cyberspace. But despite its achievements, today the UN GGE struggles to progress, not least because of some deeply held and worrisome divisions within the international community about which rules of the game should apply in cyberspace. Moreover, some UN member states are critical of subscribing to the UN GGE recommendations in which they had no

[20] Software quality assurance consists of a means of monitoring the software engineering processes and methods used to ensure quality. The methods by which this is accomplished are varied, and may include ensuring conformance to one or more standards, such as ISO 9000 or a model such as CMMI.

active stake or role. Looking ahead, it is therefore unlikely that the methods of the past will bring much change, and simply pushing for another round of negotiations now would lead to the same impasse the UN GGE currently confronts. A different process is needed. More time must be given to the UN GGE to meet in different formats with more iteration in the process, to agree on the key issues that divide nations. One way could be to create small sub-working groups that work in parallel on the most divisive topics. These working groups could interact with multiple stakeholders, including civil society and the private sector, compare notes with each other, and at the end of the road formulate a collective position on the most sensitive issues. All participants of the GMF roundtables in Paris, Warsaw, and Berlin were in favor of looking for ways that reinvigorate the UN GGE, so it may not be such a far-fledged idea.

2. Experiment with other platforms — the OECD and OSCE offer good options.

The United Nations is unique because it convenes the full spectrum of global views and interests. But there are other platforms that could be used to achieve results among a smaller group of nations. For Europe, the European Union probably offers the best perspectives. Significant progress around EU cyber safety and transparency is being made quickly, and major players like the U.K., Germany, France, Netherlands, and Poland not only increasingly share the same priorities, they now also coordinate and work together regularly. In sum, a united EU vision is steadily rising, but could be pushed further. Other organizations like the OECD or the OSCE are interesting too, because they gather a relevant number of diverse key players, their structures are more flexible, they possess a credible level of expertise, have experience working with public-private entities, and carry enough weight to negotiate on an equal footing with big countries like China, or with large institutions such as the UN or the G20. As such, the OSCE or OECD can provide their member states the opportunity to test innovative ideas around cyber security in a more controlled environment. They are also attractive from a political perspective because the negotiated rules and guidelines are non-binding. The OSCE for instance achieved remarkable results in 2016 by having its members — including Russia — agree on list of measures to reduce risk of tensions arising from cyber activities.[21] It is not unrealistic to think that ideas developed under an OECD or OSCE umbrella could then be more easily transferred to a platform like the G20, which has already made some good statements on the issue too, and where the global players could further analyze the proposals. This diplomatic sequencing could also increase the chances for successful negotiations at the level of the United Nations. So there is an opportunity to seize here.

> *"The OSCE achieved remarkable results in 2016 by having its members — including Russia — agree on list of measures to reduce risk of tensions arising from cyber activities."*

3. A rigid, binding agreement may look ideal — but accepting (some) flexibility might be more realistic

From the UN GGE to the Digital Geneva Convention, most efforts today to regulate state behavior in cyber space aim for binding commitments in the form of international law or a treaty. But some states want more flexibility, and it may be better to have them covered by something non-binding rather than have them explicitly refuse to accept a legal instrument or interpretation others have decided. The first principle of international law is that it applies only where states assent to being bound by it. Given the obvious disagreements over, and ambiguities in, the application of existing international law to offensive state behavior in cyber space, the more statements by governments, reputed lawyers, and eventually courts of international law that help build evidence toward a constructive interpretation of that law should therefore be welcomed. These can be of single governments, in bilateral agreements, or in smaller plurilateral ones, whether the G-7, EU, G-20, ASEAN, OSCE or others.

[21] OSCE Permanent Council Decision No. 1202, March 10, 2016, https://www.osce.org/pc/227281.

Moreover, a workable cyberspace agreement does not necessarily need to come in the shape of a treaty. A strong interpretation of existing law, or an expanded open-ended set of principles, or a dialogue on norms and values, is more achievable and still provides a satisfactory degree of diplomatic engagement and reassurance. The 1975 Helsinki Final Act demonstrates for instance that a broad set of principles, instead of an all-encompassing treaty with detailed legal provisions, succeeded in lessening tensions between foes and opened lines of communication between nations that do not necessarily share the same interests or values. An open set of principles may indeed help to normalize the situation in cyberspace, just like the Helsinki Final Act helped normalize European security in the years following the fall of the Soviet Union. The key to success will be for major players in cyberspace, like the Unites States, Europe, Russia, and China, to recognize a minimum common denominator in their interests and to formulate principles with an attainable level of ambition. While this may be far from the ideal scenario of binding countries to the rule of international law, working toward an open-ended agreement may be a first step toward establishing a moral and political international regime in cyberspace. Such an open ended solution should naturally not be the end destination. It should be regarded as another step toward shaping state behavior in cyber space. Looking back at the Helsinki Final Act, in fact, it served as the groundwork for the later the OSCE. Building a similar track record in cyberspace may not be unrealistic at all.

4. Create a nongovernmental organization for cyberspace whose core task will be to attribute cyber-attacks.

> *"The way forward can be to create a new, neutral nongovernmental organization that would investigate cyber-attacks and gather the necessary technical evidence to attribute them to perpetrators."*

Creating the capacity to attribute cyber-attacks is essential in order to better regulate state behavior in cyberspace. The international community has traditionally sought to sustain global peace and security by developing the capacity to attribute the use of dangerous offensive tools, from nuclear to chemical or biological weapons. Adding a cyber or ICT component would make that effort more complete. The way forward can be to create a new, neutral nongovernmental organization that would investigate cyber-attacks and gather the necessary technical evidence to attribute them to perpetrators. Its mission would only apply if civilians or civilian infrastructure have been affected by a cyber-attack during peace time. The aim of the NGO would not be to attribute cyber-attacks politically, or to respond to them, or to enforce compliance with international law. These functions should remain firmly anchored within the powers of national governments. But similar to the role played by the Organization for the Prohibition of Chemical Weapons (OPWC) in the 2018 investigation around the poisoning of former-Russian spy Sergei Skripal, the proposed nongovernmental organization for cyberspace would only collect evidence and publish the result of its analysis. Its conclusions would remain open-ended, and it would leave the formal attribution to the nation(s) that have requested the investigation. Creating such nongovernmental organization would fill an important gap by bringing together the public-private capacity for digital forensics, and by making available the experience and expertise that has already been developed in this domain. The success of such body will largely depend on its model. Just like Greenpeace in the environmental sector or Amnesty International in the human rights sector, an NGO for cyberspace would gain credibility through broad geographical representation, by adhering to transparent and accountable internal procedures, and by involving a broad base of diverse stakeholders in its activities.

There are certainly challenges to this vision. To be credible such NGO would need to deliver evidence. But the evidence in many cases would have to come from data that is delivered by governments, who are often reluctant to share information because it exposes their cyber capabilities and vulnerabilities.

Hence it is critical that an NGO for cyberspace could initially rely on the assistance of a coalition of willing nations states, but also on the input of the tech industry which has advanced systems in place to perform accurate technical attribution. A credible approach to overcome the concerns nation states may have around such organization is to think of a step-by-step implementation plan. In a first stage the NGO for cyberspace could manage a network of security researchers that focus only on the collection of information about (zero-day) software vulnerabilities and associated remedies[22]. In a second stage, once its credibility is consolidated, the competencies of the NGO could also be enlarged to include the collection of evidence. Several blueprints to create an NGO for cyberspace already exist, including reports published in 2017 by the RAND Corporation[23] and the University of Washington,[24] these can be built upon further.

> *"A coalition of countries that works together on dissuasion policies and countermeasures is likely to have more impact than one country acting alone."*

5. Dissuasion and countermeasures matter — an international coalition willing to act will make irresponsible behavior costlier.

In the absence of an overarching international treaty, national governments must think of methods to dissuade irresponsible state behavior in cyberspace, and to make it costlier to engage in malicious cyber activities. The national level in many ways will remain the most efficient responder to cyber-attacks, but the cross-border nature of cyberspace also requires governments to remain open-minded to multinational approaches to prevent and react to cyber-attacks. A coalition of countries that works together on dissuasion policies and countermeasures is likely to have more impact than one country acting alone. The 2004 Budapest Convention proves there is international appetite for such approach, as it has successfully increased cooperation among 57 nations in the fight against cyber criminality. While the scope of the Budapest Convention needs no revision, looking for similar cooperation models to address the aggressive behavior of nation states in cyberspace could be attractive. In Europe, such ambitions are already on the march. The member states of the EU adopted in June 2017 a framework for a joint diplomatic response to malicious cyber activities, the so-called EU Cyber Diplomacy Toolbox.[25] And at transatlantic level, a group of NATO allies are also aiming to agree by 2019 on a more muscular response to state-sponsored computer hackers that could involve using cyber-attacks to bring down enemy networks.[26]

An important principle behind each of these initiatives is to develop better signaling and messaging about the consequences of engaging in malicious cyber activities, and for states to agree on breeches that would trigger a collective response. This principle may not prevent nations from engaging in hostile cyber activities, but it does provide the EU or NATO member states an argument — based on the international law concept of due diligence — to call upon the nation state aggressor or its proxies to cease the behavior, and if needed to revert to countermeasures. The ongoing cooperation efforts in Europe and North-America deserve to be taken further. The EU and NATO member states could use their global partnerships in Asia, Africa or Latin-America, or leverage their relations with bodies such as ASEAN, AU, or OAS to create a broader coalition of like-minded nations that work to converge their dissuasion policies and to think together about mutually-acceptable countermeasures. If a formal agreement on this would seem too ambitious to move forward, the coalition of like-minded nations could also be forged under a more easily achievable pledge or declaration of intent. The foundation of such a declaration

[22] The model could (partially) be based on similar commercial services offered by companies like Zerodium

[23] Stateless Attribution: Toward International Accountability in Cyberspace, published by Rand Corporation, 2017

[24] Cyber Attack Attribution: A blueprint for private sector leadership, published by The Henry M. Jackson School of International Studies, University of Washington, 2017

[25] Council of the European Union - Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption, Brussels, 7 June 2017

[26] NATO mulls 'offensive defence' with cyber warfare rules, Reuters, 30 Nov 2017

could be a series of confidence-building measures among the involved nations that eliminate the risk of misinterpretation and unintended escalation in a cyber-conflict. This line could then be further developed. Nations today possess the means to construct sophisticated cyber-attacks, and it will need an equally ambitious international approach to dissuade governments from doing so. It is the only way to stabilize cyberspace.

6. The private sector is responsible for creating more security in cyberspace — but so are governments.

The industry needs to up its game as it increasingly bears the primary responsibility for responding to micro and macro-scale cyber-attacks. For ICT companies the key question remains how to close down vulnerabilities that may exist in their software systems, and what processes they have to remedy potential breaches. Nations are therefore right to demand that the private sector continuously improves product standards and assumes some responsibility for attacks that profit from weaknesses in their software. But governments must also recognize that 'security by design' is only one part of the equation. The global effects of large-scale attacks such as WannaCry or NotPetya cannot be prevented if governments rely only on product quality. Human factors, such a user system misconfiguration and poor patch management, play an equally important role in cybersecurity and can only be addressed if governments and the industry work together.

> *"Human factors, such a user system misconfiguration and poor patch management, play an equally important role in cybersecurity and can only be addressed if governments and the industry work together."*

There is more governments can do to partner with the private sector to secure cyber space. Not least, nations must continue to come together, as noted above, to strengthen the interpretation of existing and/or negotiate new legally binding rules for cyber space. But governments could also more actively support private sector initiatives that contribute to this goal. The Cyber Security Tech Accord,[27] signed in April 2018 by 34 global ICT companies, is for instance a clear signal that the private sector is willing to engage, to assume responsibility, and to adopt voluntary standards. Governments could welcome this effort by recognizing the Cyber Tech Accord's value in their national cyber security policies, by providing incentives to tech companies that decline to deliver offensive cyber capabilities to governmental clients, or by assisting the private sector to enlarge the group of companies that are involved in the Accord. That could also include non-Western ICT businesses; companies based in Russia or China could make interesting candidates. No doubt it would be a challenge to convince Russian or Chinese authorities to promote the values of the Cyber Tech Accord, but the G20 might for instance be a good platform where European or North-American governments could raise the issue. Nation states can further play their part by working with industry on two other fronts. First, by stepping away from narrow national visions and working toward an internationally accepted definition of what industry responsibility means. And second, by encouraging national administrations to set up channels that allow industry to more effectively work with governments to fight the use or misuse of vulnerabilities in software systems and to limit the extent to which governments can covertly use these. In sum, there is genuine understanding among tech companies that security in cyberspace is a matter of product quality. A strong role for the industry in cyber security is therefore acknowledged. But governments too bear responsibility. Only a shared approach, between nations and companies, will eventually provide more security in cyberspace.

[27] The content of the Cyber Tech Accord is available at https://cybertechaccord.org/

7. Private sector ideas like the Digital Geneva Conventions fulfill a need — but do not let the name distract from the substance.

Catchy tag lines are great … until they aren't. "Digital Geneva Convention" works beautifully. Many people — certainly in Europe — have heard of the Geneva Conventions; they invoke the image of law working to tame the senseless destruction of war. Evoking the creation of the International Red Cross[28] adds to that, as do references to the business community as "neutral" territory like Switzerland.

But for those working in the fields of diplomacy, international law and business, such concepts are a simplification that could prevent observers from fully understanding the nuance of some of the proposals. To many, advocating for a "new" binding international legal instrument dangerously calls into question the application of existing law; the task of drafting and ratifying a new Geneva Convention seems virtually impossible, and unnecessarily rigid. These obvious downsides related specifically to a "Convention" distract from the broader notion of the need to strengthen the international legal order to shape responsible state behavior in cyberspace, and invite criticism. Proponents of a Digital Geneva Convention increasingly understand these objections, and are beginning to talk in terms of clarifying the application of existing law to the new cyberspace realm, and developing "norms" where necessary, as important first steps perhaps leading eventually to new binding law. Indeed, this was even the tack taken in Microsoft's original June 2016 white paper on this issue;[29] it was also the approach taken in the company's contribution[30] to the November 2017 Global Conference on Cyber Space in New Delhi, which depicts a more gradualist view that more of the participants in our GMF roundtables could support.

> "The downsides related to a 'Convention' distract from the broader notion of the need to strengthen the international legal order to shape responsible state behavior in cyberspace."

8. Educate civil society — use it as a driving force in international cyber diplomacy.

Cybersecurity starts with the user. Ultimately, the user is responsible for his/her own equipment, either by regularly updating the operating system or by installing anti-virus software. However, governments and the private sector bear responsibility to make users of the internet more aware of their vulnerability in cyberspace. The most obvious tool for this is education. To be most effective, cybersecurity should be systematically included as a topic in basic and advanced education systems. Ongoing efforts in Israel could serve as an example, where the Israeli Defense Forces are working together with the different school systems to train students about cybersecurity at a very early stage of their basic education. Progress in Europe is also on the way. Germany, for instance, has recently invested significantly to improve the ICT infrastructure of its schools, and will also introduce education programs around digital awareness and concepts. But there are also opportunities at the advanced education level. The role universities can play in cyber security is still undervalued. Cyber research programs funded by governments or the private sector are still limited, and governments could also involve the scientific expertise of academia when they suspect suspicious internet activities or data.

Proper cyber education also forms the basis to inspire civil society to create grassroots movements. These civil initiatives can assist the private and public sectors in their efforts to raise awareness among internet users. But NGOs have also proven their usefulness in diplomacy and in the creation of new international laws. A classic case is the role played by six non-governmental organizations in the early 1990's that pushed for a ban on landmines,

[28] Brad Smith and Carol Anne Browne, What the Founding of the Red Cross Can Teach Us about Cybersecurity, LinkedIn, October 29, 2017.

[29] Scott Charney, Cybersecurity Norms for Nation-States and the Global ICT Industry, Microsoft blog, June 23, 2016.

[30] Kaja Ciglic, The Evolution of International Collaboration and Law Related to Cyberspace and Security, in Our Common Digital Future, The Global Conference on Cyberspace Journal, Observer Research Foundation, November 2017.

and which eventually resulted in 32 UN member states adopting in 1999 the Ottawa Mine Ban Treaty. Such capacity is still limited, but is starting to emerge on the topic of cyberspace too. The Global Commission on the Stability in Cyberspace (GCSC) has for instance demonstrated remarkable ability in exploring new norms of behavior in cyberspace. It forms an ideal platform to bring together the public and private sectors. In another case, the Tallinn Manuals are wonderfully in-depth legal analysis of the existing state of international law as it applies to the behavior of states in cyberspace. Very few other than specialized legal experts are going to read these, but parts of them can be pulled out to encourage discussion around specific ideas. Governments no longer have a monopoly on the evolution of international law, but they still don't fully utilize the potential of NGOs to develop it. The benefits of doing so could be significant.

Managing the Narrow Scope will be Key

This paper and the efforts discussed in it focuses very narrowly on only one part of the cyber security challenge — the application of international law to the (offensive) behavior of nation-states. Not all state cyber behavior is captured here. Cyber espionage, which can be deeply damaging (for instance, the Chinese attacks on the U.S. Office of Personnel Management[31]), is generally not considered a violation of sovereignty. Further, cyber-attacks — including hugely damaging ones — can come from multiple other actors, including teenagers sitting in their garages, huge organized crime rings and dangerous terrorist organizations; these too need to be addressed. That said, focusing on state behavior, and the international law that applies to it, is valid and important, even if not sufficient. This needs to be patiently but firmly explained to those countries that have a broader agenda, whether it be to undermine the multi-stakeholder governance structure of the internet or to find ways to justify internal controls on free speech. They will not be easy to convince, but the effort needs to be made.

[31] Inside the Cyber-attack that shocked the U.S. Government, *Wired Magazine*, October 23, 2016.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org